Computer Use and Misuse at the Y-12 National Security Complex

Information Technology Organization
Business Services Directorate

George A. Dailey
Chief Information Officer (CIO)
August 3, 2006

Background Information Pertaining to Work Performance on the Y-12 Site

- Y-12, as has been mentioned in the previous presentation, has many security requirements.

- Security, as it pertains to Y-12, has many implications pertaining to electronic devices to include cellular telephones and computers.

- **The major telecommunications issue affecting performance by Y-12 subcontractors is:**

IMPROPER USE OF

CELLULAR TELEPHONES!

Camera-Equipped and Other Feature-Laden Cellular Telephones are a Y-12 Threat

- Cellular telephone subscribers, at the end of calendar 2005, numbered 207.9 million (69% of the population) within the U.S. (http://files.ctia.org/pdf/Wireless_Quick_Facts_April_06.pdf)
  - Cellular telephones have become common accessories for U.S. citizens and are usually not considered improper when visiting work sites, or not considered at all
- “Camera-enabled phones are taking the market by storm, growing from 6% of all handsets made in 2002, to 16% in 2003, to 32% in 2004, and to a projected 65% in 2007…”
  - Cameras have never (since Y-12 founded in 1943) been allowed at or within Y-12 without prior permission
- In General:

DO NOT CARRY ON YOUR PERSON OR USE CELLULAR TELEPHONES AT THE SITE WITHOUT FIRST READING ASSOCIATED SECURITY REQUIREMENTS AND OBTAINING PROPER AUTHORIZATION!

Y-12 Cellular Telephone Possession Guidance

- No: Y15-404 (Acceptable Use of Information Technology Equipment), Rev. Date: 11/21/05, APPENDIX E

  CELLULAR TELEPHONES – Acceptable Use Instructions and Other Information (Page 1 of 1)
- Use of personal cellular phones is prohibited within the Y-12 NSC legal boundary (i.e., 229 Boundary or the “blue” line) unless prior approval through the Y-12 Telecommunications Process (TP). For practical application, employees may consider this boundary to be the first external badge checkpoint on Bear Creek Road and New Hope Pond Road.
- Personal cellular telephones must not be used and must remain in the employee's vehicle inside the 229 boundary. Additionally, if an authorized vehicle is driven into the fenced property protection areas of Y-12, any personal cellular phone within the vehicle must be secured (e.g., within the glove box or other similar storage area) and must remain within the vehicle at all times.
- In the case of a personal emergency while within the Y-12 NSC boundary, a personal cellular phone may be utilized to contact the Plant Shift Superintendent’s office at 574-7172 for assistance.

Obtaining Permission for Cellular Telephone Use Begins with Procurement

- In extenuating circumstances pertaining to personal situations requiring personal cellular telephone use, exceptions to this guidance may be requested. The exception request, review, and conclusion process with written approval must be completed prior to taking exception (i.e., personal cellular telephone use within the 229 boundary or within leased/rented space) to this guidance. The exception request must be made to the Y-12 Chief Information Officer (E-mail UID: CIO) who will coordinate review and request closure among the responsible oversight divisions.
- **For subcontractors/contractors, contact must begin with the Procurement Organization Buyer who placed your contract.**
- Conscious misuse of this policy will result in security action including issuance of a security infraction and possible subcontract action up to and including termination.

Computer Usage at Y-12 is Monitored at All Times

- Whether it is a BWXT Y-12 provided computer or your business computer authorized for Y-12 use, **all computing activities at Y-12 are monitored all the time.**
  - There should be no expectation of privacy when using the Y-12 computing resources.
- After cellular telephones, mis-use of computing resources at Y-12 is the second largest problem for subcontractors.
- There is an expectation that computing use is business related.
  - E-mail: E-mail should only be used for content that the sender would be comfortable entering into the public record. As a responsible member of the Y-12 community, users are expected to apply common sense and civility to the use of e-mail. Use of e-mail is expected to be legal, ethical, and responsible.
  - Internet: **All Internet use is monitored all the time.**
    - Y-12 monitors inbound and outbound Internet use by: User ID, including the time of each internet “hit”, what Web site was visited, and the “browse” or online time for each session.
    - Y-12 blocks some inappropriate Web sites, but records each site that a user tries to access, even if they were blocked by the Y-12 filters.

Why Does Y-12 Review Internet Use So Strongly?

RISK

Security Risk

- Peer-to-Peer (P2P) File Sharing
- Instant Messaging
- Employee Hacking
- Spyware

Legal Liability

- Pornography
- Peer-to-Peer (P2P) File Sharing
- Instant Messaging

Bandwidth Misuse

- Streaming Media
- Peer-to-Peer File Sharing
- Internet Radio & TV

Productivity

- Instant Messaging
- PC Gaming

CORPORATE AMERICA

- **1 in every 5 corporate employees use a public IM tool to chat.**
- **70+% of hacking exploits are from the inside.**
- **90% corporate PCs have Spyware.**

- **73% of P2P searches are for pornography.**
- **45% of P2P downloads contain malicious code.**

- **44% of employees actively use streaming media.**

- **An average employee loses 6.5 hours of productivity a week.**

* Source: Websense, Kathy Butler Presentation, August 27, 2003

Y-12 Internet Policies Benefit Versus Corporate America

RISK	Y-12
Security Risk – Peer-to-Peer (P2P) File Sharing – Instant Messaging – Employee Hacking – Spyware	– **Instant Messaging (IM) not allowed.** – **No inside hacking attacks.** – **<1% of site PCs have Spyware.**
Legal Liability – Pornography – Peer-to-Peer (P2P) File Sharing – Instant Messaging	– **Pornography is blocked.** – **P2P blocked, stopping malicious software downloads.**
Bandwidth Misuse – Streaming Media – Peer-to-Peer File Sharing – Internet Radio & TV	– **Streaming media is blocked.**
Productivity – Instant Messaging – PC Gaming	– **Average employee loses few or no minutes of productivity/week.**

Other Computing Resource Use Considerations

- **Personal Data Assistants (PDAs):** also called personal electronic devices (PEDs) such as BlackBerry, Piarea, Hewlett- Packard (HP) Palmtop Computer, and HP Jornada Palmtop – regardless of ownership – are prohibited unless pre-approved through the Y-12 Telecommunications Proposal approval process.
  - **Use of Privately-owned PDAs** - Privately-owned PDAs (even those with no wireless capability) must be approved on a case-by-case basis through the Telecommunications Proposal approval process for use in Y-12 NSC owned, leased, or rented space. These units cannot have voice recording capability enabled. No privately-owned PDAs may be connected to the Y-12 networks including medical purpose PDAs, such as devices which measure insulin levels for diabetics.

Other Computing Resource Use Considerations continued

- **No wireless devices can be used at the Y-12 NSC without prior approval through the Telecommunications Proposal approval process.**
  - Portable electronic devices capable of recording information or transmitting data (e.g., radio frequency, infrared, and/or data link electronic equipment) are considered controlled items and are NOT permitted in Limited, Exclusion, Protected, or Material Access Areas without special authorization and approval, fully justified need, and proper control of their use and availability.
  - External companies listed on Post Orders as being allowed access to the Y-12 NSC <u>are approved</u> to bring electronic devices such as special purpose barcode readers, tablet PDAs, and other similar inventory collection devices into the plant in their vehicles for the purpose of recording delivery and other inventory information.

Other Computing Resource Use Considerations continued

- **Flash Memory Devices (e.g., “thumb” drives, etc.)**
  - With the miniaturization of memory devices, additional security measures are necessary to protect IT and data in Y-12 NSC. Any memory device [such as Universal Serial Bus (USB) flash memory drives, USB keys, memory sticks, etc.] used within Y-12 NSC owned, leased, or rented facilities must meet all applicable guidelines for AIS storage media handling including the requirements for proper labeling, marking, accountability, and destruction. Please discuss this topic with your Procurement Division buyer if you require use of such a device.
  - Discovery of memory devices in use within Y-12 NSC owned, leased, or rented space not meeting company requirements for use, storage, and labeling will be considered to be a breach of security and will result in the possible issuance of a security infraction, possible criminal liability for unauthorized disclosure, and disciplinary action up to and including termination.

Y-12 Has Significant Computing Resources to Expedite Your Work

- Y-12 computing resources are significant.
  - If your staff are assigned to or your approved computing equipment connected to Y-12 computing resources, you will find them robust and enabling.
  - The computing support staff are knowledgeable, helpful, and available to answer questions.
  - If you adhere to Y-12 computing policies, you and/or your staff will work without hindrance and with confidence that the computing infrastructure will be available as needed.
- Unauthorized and/or improper computing/electronic infrastructure activity is quickly recognized and mitigated.
- We want our shared work to be productive to all parties with the computing/electronic environment viewed as a capable, reliable work enabler.